View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

ADVANCES IN APPLIED MATHEMATICS 7, 101–122 (1986)

A Random Walk in Higher Arithmetic

D. V. CHUDNOVSKY* AND G. V. CHUDNOVSKY*

Department of Mathematics, Columbia University, New York, New York 10027

DEDICATED TO HERBERT ROBBINS ON THE OCCASION OF HIS 70TH BIRTHDAY

A random walk technique is applied to linear differential equations. © 1986 Academic Press, Inc.

INTRODUCTION

The higher arithmetic is the arithmetic of algebraic number fields and their transcendental extensions, generated by constants of classical analysis and algebraic geometry. Such constants are typically values of classical special functions, defined by particular differential equations. Say, periods of algebraic varieties are given by definite integrals of algebraic functions, and sometimes they are expressed in terms of hypergeometric functions. (For one example of a class of periods of algebraic varieties and their relationship with the Dirichlet series and p-adic linear differential equations see Cassou-Noguès [1].) A typical problem of higher arithmetic is the problem of transcendence or algebraicity on an arithmetically interesting value of a particular special function, usually at an algebraic point. For example, is $\Gamma(1/5)$ transcendental? Is $\zeta(3)$ transcendental? Is e^{π}/π rational? Is $e + \pi$ rational?

These (transcendental) problems do not belong to the realm of distribution problems of analytic number theory (additive number theory or representation problems), where probabilistic methods are common. Probabilistic methods are applied in additive number theory usually in the form of ergodic properties of various transformations on lattices (tori) constructed directly in algebraic number fields under consideration. In transcendental problems, when we want to prove or disprove the transcendence of a value

*This work was partially supported by the U.S. Air Force under Grant AFOSR-81-0190 and by the National Science Foundation under Grant MCS-82-10292.

0196-8858/86 $7.50
Copyright © 1986 by Academic Press, Inc.
All rights of reproduction in any form reserved.

of a function, no such structure, to which probabilistic methods can be applied, exists *a priori*. Nevertheless, as we shall see, one can construct a random walk generated by orders of zeroes of a certain approximation to the function, whose value we are considering. In other words, in a completely deterministic situation, when one wants to prove that a value $f(x_0)$ of an analytic function $f(x)$ at an algebraic point $x = x_0$ is transcendental, one encounters a random process. This process represents a system of Markov-type equations or inequalities on orders of zeroes of approximations (usually, it is rational, Padé or an algebraic approximation) to the function $f(x)$. Though we do not know the exact orders of zeroes of these approximations, the inequalities between them are sometimes sufficient to deduce the desired transcendence of $f(x_0)$. We call such a Markov chain a "random walk" on a zero-set of an approximation function.

Methods of random walks on a zero-set were introduced for the first time in [2, 3]. Later these methods were applied in the graded Padé approximation technique to prove the best diophantine approximation results for values of solutions of linear differential equations at algebraic points (see the exposition in [4]). We introduce a random walk on a zero-set from [2, 3] in Section 1 together with the sketch of the proof of an important transcendence criterion formulated in terms of superharmonic functions. Random walks of Section 1 are traditional symmetric one-step random walks on integral lattices $\mathbb{Z}^m$. Our new result requires a different version of a random walk, generated by Möbius transformations with integral coefficients acting on the upper half plane H. From the abstract, group theoretic point of view (cf. [5]), such a random walk corresponds to a particular version of a random walk on a free group, generated by two elements, in the representation of this group via the full modular group $\Gamma(1) = SL_2(\mathbb{Z})$ acting on H. This visually unusual non-Euclidean random walk is applied in Section 2 to another problem of higher arithmetic: how to distinguish transcendental functions from algebraic ones. A hypothetical answer to this problem for functions defined by linear differential equations with rational function coefficients is given by the Grothendieck conjecture [6, 7]. The Grothendieck conjecture tests for the existence of sufficiently many polynomial solutions mod p of linear differential equations for a variety of primes p. Recently we have verified the Grothendieck conjecture for one class of linear differential equations, including the Lamé equations [8, 9] using Padé approximation methods. Here we combine Padé approximation techniques with a non-Euclidean random walk on a zero set to prove the Grothendieck conjecture for a new class of linear differential equations, called algebraically represented (see Sect. 2; roughly speaking this means that a monodromy group of a differential equation has a matrix representation over $\overline{\mathbb{Q}}$). As an auxiliary result we present a simple but useful method of reduction of an arbitrary linear differential equation over $\overline{\mathbb{Q}}(x)$ to a linear differential equation (of a

higher order) with singularities at $0, 1, \infty$ only. This method, based on Belyi's observation [10], allows us to uniformize solutions of linear differential equations over $\overline{\mathbf{Q}}(x)$ by means of single valued functions in H and to introduce a random walk there. The uniformizations of linear differential equations is an interesting subject in itself and its various connections with the accessory parameters problem will be treated in detail elsewhere. Our results on the proof of the Grothendieck conjecture can be reformulated to imply transcendence results for numbers. One of them shows that, starting from an arbitrary transcendental G-function [11] solution of a linear differential equation over $\overline{\mathbf{Q}}(x)$, its analytic continuation along closed paths in $\mathbf{CP}^1$ generate at least one transcendental number.

A truly random walk on the field of higher arithmetic would reveal a much richer structure than that indicated here. It would touch the distribution problem for traces of Frobenius of algebraic varieties and their applications. But a random walker takes too long to visit all cities. We will continue our random promenade in this field as well as in others enviously following the pattern of Herbert Robbins.

1. We use standard definitions on the random walk on m dimensional lattices [5].

By a random walk on an m-dimensional lattice $\mathscr{L} = \mathbf{Z}\mathbf{e}_1 \oplus \cdots \oplus \mathbf{Z}\mathbf{e}_m$, one understands a motion of a particle on $\mathscr{L}$, when a particle moves from its present position to the one of $2m$ neighboring positions with equal $(= 1/2m)$ probability, independent of its position in the previous moments of time. It is easier to use the language of potential theory and a discrete analog of the Laplace operator $(1/2)\Delta_m$ $(= (1/2)\sum_{i=1}^{m} \partial^2/\partial x_i^2)$:

$$A_m \circ f(x) = \frac{1}{2m} \sum_{i=1}^{m} f(x + \mathbf{e}_i) - f(x)$$

(for $x \in \mathscr{L}$). As usual, we call a function $f(x)$ on $\mathscr{L}$ a harmonic function, if $A_m f = 0$ and superharmonic, if $A_m f(x) \leq 0$ (for all x). As the theory of Newton potential shows, harmonic functions on $\mathscr{L}$ in dimensions $m = 1$ or $m = 2$ are only constant ones, and for dimensions $m \geq 3$ there is a large supply of harmonic functions. As in probability theory, in number theory one is interested only in nonnegative superharmonic functions, called excessive. As we shall see, superharmonic functions arising from transcendence problems satisfy a strong inequality $Af(x) \leq -\varepsilon f(x)$ for some $\varepsilon > 0$, and can be defined only on a small subdomain of $\mathscr{L}$.

Looking for the transcendence result takes often a long random walk. If we were to walk long enough the following theorem appears:

THEOREM 1.1 [2]. *Let $f(z)$ be a transcendental (i.e., not an algebraic over $\overline{\mathbf{Q}}(z)$) meromorphic function of finite order growth $\leq \rho$. Then there are* at most ρ *algebraic numbers z_0 such that $\partial^k f(z)/\partial z^k|_{z=z_0} \in \mathbf{Z}$ for all $k \geq 0$.*

Here the function $f(z)$ is meromorphic of order $\leq \rho$, if $f(z) = g(z)/h(z)$, where $g(z)$ and $h(z)$ are entire functions in $\mathbf{C}$ and

$$\max_{|z|=R} \{|h(z)|, |g(z)|\} \leq \exp\{c_0 R^{\rho}\}.$$

Theorem 1.1 is but a simple example of a kind of transcendence result. For example, the same method of a random walk on a zero set as used in the proof of Theorem 1.1, but for a different lattice, lead to the following multidimensional result:

THEOREM 1.2 [3]. *Let $f(\bar{z})$ be a transcendental meromorphic function in $\mathbf{C}^n$ of the order of growth at most ρ. Then the set of all points $\bar{z}_0 \in \mathbf{C}^n$ such that $\partial_{z_1}^{k_1} \cdots \partial_{z_n}^{k_n} f(\bar{z}_0) \in \mathbf{Z}$ for all $k_i \in \mathbf{Z}$, $k_i \geq 0$, is contained in an algebraic hypersurface in $\mathbf{C}^n$ of degree at most $n\rho$.*

Remark. In Theorems 1.1 and 1.2, one can replace $\mathbf{Z}$ by a ring of integers in an imaginary quadratic field. Also the dependence on n of the degree in Theorem 1.2 can be significantly improved [3].

There are versions of Theorems 1.1 and 1.2 that deal with the simultaneous integrality (algebraicity) of derivatives of two or more meromorphic functions, under various additional conditions (e.g., see [12]). However, Theorems 1.1 and 1.2 are the best possible results of their kind.

For example, to prove the transcendence of π, it is sufficient to put $f(z) = e^z$ in Theorem 1.1. (One sees that for $f(z) = e^z$, $\rho = 1$, and $z_0 = 0$ gives $e^{z_0} \in \mathbf{Z}$. Thus for *any* algebraic $z_0 \neq 0$, $e^{z_0} \notin \mathbf{Z}$. Hence $2\pi i$, and thus π, cannot be an algebraic number.) Similarly, Theorems 1.1 and 1.2 can be used to prove transcendence results for constants connected with elliptic functions, including periods and quasi-periods of elliptic curves defined over $\overline{\mathbf{Q}}$, and values of elliptic integrals of the first, second, and, sometimes, the third kind. In this relation it should be remarked that many transcendence statements can be reduced to the form of Theorem 1.1, which speaks only of integrality of values of functions. (E.g., when one studies the algebraicity of values of the Weierstrass elliptic functions $\mathscr{P}(u)$ with algebraic invariants g_2 and g_3, one has to consider functions of the form $f(\bar{z}) = A\prod_{i=1}^{n}(\prod_{j=1}^{d}\mathscr{P}^{(j)}(z_i))$ for an appropriate integer A and functions $\mathscr{P}^{(j)}(u)$ having invariants $g_2^{(j)}$ and $g_3^{(j)}$, conjugate to g_2 and g_3). To prove Theorem 1.1, one tries to construct algebraic approximations to the function $f(z)$ at all points $z = z_0$ for which $\partial^k f(z)/\partial z^k|_{z=z_0} \in \mathbf{Z}$. Let us denote the set of such algebraic points z_0 by S, and let us *assume*, contrary to Theorem 1.1, that

$$\mathrm{Card}(S) > \rho.$$

We imbed a finite set S into a Galois algebraic number field K (Galois means that every conjugate to an element of K is also an element of K).

The only way to prove a result like Theorem 1.1 is to pass from an algebraicity statement for numbers $\partial^k f(z)/\partial z^k|_{z=z_0}$ and z_0 to an algebraicity statement for functions. Thus, we have to prove that an assumption $\mathrm{Card}(S) > \rho$ forces $f(z)$ to become an algebraic function. To prove that $f(z)$ is an algebraic function we have to exhibit an algebraic relation between z and $f(z)$. We are trying to construct this relation by looking at a polynomial $P(z, f(z))$ that has a lot of zeroes at points $z = z_0 \in S$.

The polynomial $P(z, f(z))$ defines algebraic approximations of $f(z)$ at $z = z_0 \in S$, the approximations being algebraic functions $f_{\mathrm{app}}(z)$, such that $P(z, f_{\mathrm{app}}(z)) \equiv 0$. We want to show that these approximations are "too good," i.e., $f(z) = f_{\mathrm{app}}(z)$ or $P(z, f(z)) \equiv 0$.

Thus our auxiliary function (an approximating function) has the form

$$F(z) \stackrel{\mathrm{def}}{=} P(z, f(z)). \tag{1.1}$$

Here $P(x, y)$ is a polynomial from $\mathbb{Z}[x, y]$ (with rational integral coefficients) such that

$$\begin{aligned} \deg_x P(x, y) &\le L \cdot (\log L)^{-1/4} \\ \deg_y P(x, y) &\le (\log L)^{3/4}. \end{aligned} \tag{1.2}$$

Here L is a parameter representing a sufficiently large integer determining lower bounds on orders of zeroes at $z = z_0 \in S$ of approximations.

It is an easy consequence of the Dirichlet's box principle that there exists a polynomial $P(x, y) \in \mathbb{Z}[x, y]$ satisfying (1.2) and such that the function $F(z)$ in (1.1) satisfies the following conditions:

$$F^{(k)}(z_0) = 0 \tag{1.3}$$

for any $z_0 \in S$ and $k = 0, \ldots, L$.

To see why such $P(x, y)$ exists, one should look at conditions (1.3). Each of the conditions (1.3) represents a linear equation on coefficients of polynomial $P(x, y)$ considered as undetermined integers. This way we obtain from (1.3) a system of $(L + 1)\mathrm{Card}(S)$ linear equations on undetermined coefficients of $P(x, y)$, whose number is $L(\log L)^{1/2} \gg (L + 1)\mathrm{Card}(S)$, for L being sufficiently large. Thus a nontrivial solution to (1.3) exists. Moreover, the Dirichlet's box principle implies that the coefficients of $P(x, y)$ can be found to be in absolute value at most

$$\exp\bigl(c_1 L(\log L)^{1/2}\bigr).$$

Results weaker than Theorem 1.1 were proved a long time ago, starting from Schneider, Straus, and Lang. However, their distinct feature, absent here, was the dependence of cardinality of S not only on ρ, as in Theorem 1.1, but also on the degree of the field K, where S lies. Typically the standard proof is based on the estimate from above of $|\alpha|$ for $\alpha = F^{(u_0)}(z_0)$, where u_0 is the order of zero of $F(z)$ at $z = z_0$ (and $u_0 < \infty$ means that $F(z) \not\equiv 0$). If $K = \mathbb{Q}$ and z_0 is a rational number, then the upper bound on $\alpha = F^{(u_0)}(z_0)$ would be sufficient to end the proof, because $|\alpha|$ is very small, but $\alpha \neq 0$ and $\mathrm{denom}(z_0)^{\deg_x(P)}\alpha$ is a nonzero rational integer. Then $|\alpha| \geq \mathrm{denom}(z_0)^{-\deg_x(P)}$—an apparent inconsistency with the (stronger) upper bound on $|\alpha|$. However, if $\alpha \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$ and $[K : \mathbb{Q}]$ is large, these arguments are not sufficient to end the proof ($F(z) \equiv 0$ or $u_0 = \infty$), because $|\alpha|$ can be very small even for an integral $\alpha \in K$, but still be non-zero. It is at this point that we introduce a random walk on a lattice associated with S and K.

Let G be a Galois group of K (so that the degree of K over $\mathbb{Q}$ is equal to the order of G).

Let $\mathrm{Card}(S) = n$, $S = \{z_1, \ldots, z_n\}$. The lattice, on which we consider superharmonic functions is

$$\mathbb{Z}^J, \qquad \text{where } J = (G \setminus \{1\}) \times \{1, \ldots, n\}.$$

We take a standard basis in $\mathbb{Z}^J$: $\mathbf{e}(j)$: $j \in J$

$$\mathbf{e}(j)[j_1] = \delta_{j, j_1} : j, j_1 \in J.$$

The lattice $\mathbb{Z}^J$ is mapped into a lattice in K, generated by elements of S and their conjugates. Namely,

$$\text{if } \mathbf{n} = \left(n_{(g,i)} : g \in G \setminus \{1\}, 1 \leq i \leq n\right) \in \mathbb{Z}^J,$$

then we put

$$\lambda(\mathbf{n}) \overset{\text{def}}{=} \sum_{i=1}^{n} \sum_{g \in G} n_{(g,i)} \cdot z_i^{(g)}, \tag{1.4}$$

where $z_i^{(g)}$ is a conjugate to z_i under the action of an automorphism $g \in G$ (and for $g = 1 \in G$ one puts $n_{(1,i)} \overset{\text{def}}{=} -\sum_{g \in G \setminus \{1\}} n_{(g,i)}$: $i = 1, \ldots, n$).

Next, we consider together with $F(z)$, the "shifted functions":

$$F_{\mathbf{n}}(z) \overset{\text{def}}{=} P(z + \lambda(\mathbf{n}), f(z)) \tag{1.5}$$

for any $\mathbf{n} \in \mathbb{Z}^J$.

The main algebraic relation between "shifted functions" $F_{\mathbf{n}}(z)$ has the form:

For any $k \geq 0$ and $i = 1, \ldots, n$, the number $F_{\mathbf{n}}^{(k)}(z_i)$ (from K) is algebraically conjugate to $F_{\mathbf{m}}^{(k)}(z_i)$, where $\mathbf{m}$ is a "neighbor" of $\mathbf{n}$ in $\mathbb{Z}^J$.

Combining these algebraic relations between $F_{\mathbf{n}}^{(k)}(z_i)$, with Jensen's formula for $\log|F_{\mathbf{n}}|_R$ in terms of zeroes of $F_{\mathbf{n}}(z)$, we obtain the following system of inequalities on orders of zeroes of $F_{\mathbf{n}}(z)$ at $z = z_i \in S$.

If $u_i^{\mathbf{n}}$ (for $\mathbf{n} \in \mathbb{Z}^J$, $i = 1, \ldots, n$) denotes the order of zero of $F_{\mathbf{n}}(z)$ at $z = z_i$, then we have:

$$d(\rho - 1)u_i^{\mathbf{n}} \geq \sum_{j=1,\, j\neq i}^{n} u_j^{\mathbf{n}} + \sum_{j=1,\, j\neq i}^{n} \sum_{g\in G\setminus\{1\}} u_j^{\mathbf{n}+\mathbf{e}(g,j)-\mathbf{e}(g,i)}; \quad (1.6)$$

$\mathbf{n} \in \mathbb{Z}^J$, $i = 1, \ldots, n$.

Here $d = \mathrm{Card}(G)$, $n = \mathrm{Card}(S) > \rho$ (according to our assumptions). Thus we arrived at a scheme of a "random walk" in $(d-1)n$-dimensional lattice. The essential feature, distinguishing (1.6) from the usual random walk schemes, is that on the right-hand side of (1.6) there appear $d(n-1)$ summands and on the left-hand side of (1.6), when $\rho < n$, the constant $d(\rho - 1)$ is less than $d(n-1)$.

Thus, we are lead to nonnegative superharmonic functions, satisfying conditions of the type:

$$Af(x) \leq -\varepsilon f(x) \quad (1.7)$$

for some $\varepsilon > 0$. Our functions are definitely nonnegative because they represent orders of zeros of regular functions. Also, at the origin, our function is definitely positive by the construction and (1.3). It turns out that for every $\varepsilon > 0$ and any $m \geq 1$, functions satisfying (1.7) can be positive *only* in a cube is $\mathbb{Z}^m$, containing the origin, *if* the size of the cube is *less* than a constant $c_2(m, \varepsilon)$. Consequently, there is no nonnegative solutions of (1.7) in the whole lattice, and $\mathrm{Card}(S) = n \leq \rho$ always. This proves Theorem 1.1.

Simultaneously, we are lead to a new class of excessive functions. For $m \geq 3$, we do not know the maximal side of a cube in $\mathbb{Z}^m$, where a nonnegative solution of (1.7) can exist.

This example is a typical illustration of a random walk on a zero set, where orders of zeroes of different "approximations" at different points generate probabilistic distribution. The goal of proving transcendence is often achieved, if this distribution only has finite support.

2. The next application of random walks deals with the non-Euclidean zero-set. This kind of random walk turns out to be crucial in the

solution of another transcendental problem of higher arithmetic: how to tell the transcendental characteristics of a manifold with a connection, from finite (mod p) arithmetic information. Plainly speaking, can one determine a monodromy group of a linear differential equation (typically given by matrices with transcendental number entries) by the properties of this differential equation after its reduction mod p for many (several) primes p. For example, is it possible to tell whether all solutions of a linear differential equation are algebraic just by examining this equation mod p? Grothendieck formulated a conjecture that answers this question [6, 7] and Katz [6] extended this conjecture and showed how from the universal truth of the Grothendieck conjecture it follows that one can determine the Lie algebra of the monodromy (Galois) group of a linear differential equation from certain mod p characteristics of a linear differential equation (p-curvature matrices). Thus, the main problem is to prove the original Grothendieck conjecture, which we are about to formulate.

Let K be an algebraic number field and for a prime ideal $\mathscr{P}$ of K, $\bar{K}_{\mathscr{P}}$ denotes the residue field of K (mod $\mathscr{P}$). Also we denote by k, a field of characteristic $p > 0$, by $k[x]$, the ring of polynomials in x over k, by $k[[x]]$, the ring of formal power series in x over k, and by $k(x)$ and $k((x))$, respectively, the quotient fields of $k[x]$ and $k[[x]]$. We consider $k((x))$ to be a differential field with the standard differentiation in x: $\alpha' = 0$ for $\alpha \in k$ and $(x^n)' = n \cdot x^{n-1}$. Consequently, the field of constants of $k((x))$ is $k((x^p))$.

We start with a linear differential equation over $K(x)$:

$$a_n(x)y^{(n)}(x) + \cdots + a_1(x)y'(x) + a_0(x)y(x) = 0, \qquad (2.1)$$

$a_i(x) \in K[x]$ $(i = 0, \ldots, n)$ and its reductions (mod $\mathscr{P}$) in $\bar{K}_{\mathscr{P}}(x)$, denoted by $(2.1)_{\mathscr{P}}$.

Clearly, if $(2.1)_{\mathscr{P}}$ has a solution in $\bar{K}_{\mathscr{P}}((x))$, then, after multiplication by a constant, it has a solution in $\bar{K}_{\mathscr{P}}[[x]]$.

We say that the equation $(2.1)_{\mathscr{P}}$ has sufficiently many solutions, if $(2.1)_{\mathscr{P}}$ has n linearly independent solutions in $\bar{K}_{\mathscr{P}}[[x]]$.

For scalar (linear) differential equations (2.1) the Grothendieck conjecture reads:

The Grothendieck Conjecture. Let for almost all prime ideals $\mathscr{P}$ of K, $(2.1)_{\mathscr{P}}$ have n solutions in $\bar{K}_{\mathscr{P}}(x)$, linearly independent over $\bar{K}_{\mathscr{P}}(x^p)$, i.e., let $(2.1)_{\mathscr{P}}$ have sufficiently many solutions for almost all $\mathscr{P}$. Then all solutions of (2.1) are algebraic functions.

The Grothendieck conjecture can be also formulated for matrix linear differential equations in terms of p-curvature operators Ψ_p [6]. Let us consider an arbitrary matrix linear differential equation with coefficients

from $K(x)$:

$$\left(\frac{d}{dx}I + A(x)\right)\bar{f}^t = 0, \tag{2.2}$$

for $I_{i,j} = \delta_{i,j}$ and $A(x) \in M(n, K(x))$. The p-curvature operator Ψ_p of (2.2) (mod p) is

$$\Psi_p = \left(\frac{d}{dx}I + A(x)\right)^p \pmod{p}.$$

In fact, Ψ_p is a linear operator [6, 7] and $\Psi_p = A_p \pmod{p}$, where A_n are defined inductively as follows:

$$A_1 = A(x), \qquad A_{n+1} = d/dx A_n + A_n A_1 (n \geq 0).$$

THE GROTHENDIECK CONJECTURE. If for almost all p, p-adic curvature operator Ψ_p of (2.2) is zero, $\Psi_p = 0$, then all solutions of the equation (2.2) are algebraic functions.

Similar p-curvature invariants exists for scalar linear differential equations (2.1), where they can be defined as $(d/dx)^p \bmod K_{\mathscr{P}}(x)[d/dx] \cdot L_{\mathscr{P}}$ for an appropriate linear differential operator $L_{\mathscr{P}} = \sum_{i=0}^{n} a_i(x)(d/dx)^i \bmod \mathscr{P}$.

It is known that equations satisfying the assumptions of the Grothendieck conjecture possess important properties:

PROPOSITION 2.1 (KATZ [6, 7]). *If Eq.* $(2.1)_{\mathscr{P}}$ *has sufficiently many solutions for infinitely many prime ideals* $\mathscr{P}$ *of* K, *then* (2.1) *is a Fuchsian linear differential equation. If* $(2.1)_{\mathscr{P}}$ *has sufficiently many solutions for almost all* $\mathscr{P}$, *then all exponents at regular singularities of* (2.1) *are rational numbers and the local monodromy of* (2.1) *is finite and cyclic in the neighborhood of any point.*

Katz proved the truth of the Grothendieck conjecture for the class of Picard–Fuchs equations (i.e., deformation equations for the periods of algebraic varieties), including hypergeometric function equations. In [8, 9] we proved the Grothendieck conjecture for a large class of differential equations, including Lamé equations and arbitrary rank one equations over algebraic curves of positive genus. These results were accomplished using the combination of Padé approximation methods with a particular form of the converse to the Eisenstein theorem. The Eisenstein theorem states that for an expansion of $f(x) = \sum_{n=0}^{\infty} a_n x^n$ of an algebraic function $f(x)$ over $\overline{\mathbf{Q}}(x)$, there exists an integer $D \geq 1$ such that $D^n \cdot a_n$ is an integer for all $n \geq 0$. Our result from [9, Theorem 5.2] is a converse to the Eisenstein theorem, proved under the assumption that the function $f(x)$, whose power

series expansion is integral is parametrized by meromorphic functions of finite order of growth. This assumption of uniformization by means of meromorphic functions also holds for results from [9] on the Grothendieck conjecture. Not all solutions of linear differential equations can be uniformized this way, and automorphic functions for groups of Möbius transformations of the upper half plane H have to be used for the uniformization.

We can prove the Grothendieck conjecture, using the non-Euclidean random walk, for the class of linear differential equations whose monodromy group admits an "algebraic representation."

Let us recall first of all the definition of the monodromy group. For a linear differential equation

$$a_n(x)y^{(n)}(x) + \cdots + a_0(x)y(x) = 0, \tag{2.1}$$

with $a_i(x) \in \overline{\mathbf{Q}}(x)$ $(i = 0, \ldots, n)$, let $y_1(x), \ldots, y_n(x)$ be a fixed fundamental system of solutions of (2.1). Then for a closed path γ, not containing the singularities of (2.1) and analytic continuation of $(y_1(x), \ldots, y_n(x))$ from x to x along γ implies a linear transformation:

$$(y_1, \ldots, y_n)^t \underset{\gamma}{\mapsto} M_\gamma \cdot (y_1, \ldots, y_n)^t,$$

where the (constant) matrix $M_\gamma \in GL_n(\mathbf{C})$ is called a monodromy matrix of (2.1) (corresponding to γ). The set of all matrices M_γ generates a *monodromy group* of (2.1), which is a representation of the fundamental group $\pi_1(\mathbf{CP}^1 \setminus S_0)$, where S_0 is the set of all singularities of (2.1). A monodromy group of (2.1) dependes on the choice of the fundamental system of solution of (2.1), and, invariantly, is defined only as a conjugacy class in $GL_n(\mathbf{C})$. We call an equation (2.1) algebraically represented if (2.1) has a monodromy group which is a subgroup of $GL_n(\overline{\mathbf{Q}})$, i.e., the monodromy matrices have algebraic entries only. For such a class of linear differential equations we can prove the Grothendieck conjecture:

THEOREM 2.2. *Let us assume that the equation* (2.1) *be algebraically represented, i.e.,* (2.1) *has a monodromy group which is a subgroup of* $GL_n(\overline{\mathbf{Q}})$. *If for almost all prime ideals* $\mathfrak{P}$ *the equation* $(2.1)_{\mathfrak{P}}$ *has n linearly independent solutions mod* $\mathfrak{P}$, *then all solutions of* (2.1) *are algebraic functions.*

Remark. The assumption of algebraic representation of a monodromy group of (2.1) is reasonable, because whenever (2.1) has only algebraic function solutions, its monodromy group is a representation of a subgroup of a symmetric group, and thus the equation is algebraically represented.

The class of algebraically represented equations includes many classical equations (like hypergeometric ones), but has an empty intersection with the

class of equation for which the Grothendieck conjecture was proved in [9]. For equations from [9] the monodromy group was not algebraically represented because elements of the monodromy matrices were built from periods of Abelian integrals of the first, second, and third kind. In fact, the transcendence of some of the elements of the corresponding monodromy group follows from the results of [9] as well. As compared with [9], Theorem 2.2 is a more delicate transcendence statement. Also, Theorem 2.2 provides one with a computational method to check for the algebraicity of solutions of (2.1). If one sees, say numerically, that the elements of the monodromy group of (2.1) are transcendental quantities, then (2.1) does not have algebraic solutions only, (and, most likely, does not satisfy even the assumptions of the Grothendieck conjecture). On the other hand, if, numerically, elements of the monodromy matrices of (2.1) are algebraic quantities, Theorem 2.2 tells us unconditionally that it is sufficient to verify the assumptions of the Grothendieck conjecture. In this relation we want to state that Theorem 2.2 is an effective statement in the sense that, to insure the algebraicity of all solutions of (2.1), it is sufficient to check the assumptions of the Grothendieck conjecture only for a finite effective set of primes p. Namely, for an algebraically represented equation (2.1), and any $M > 0$, there exists an effective P, depending only on M and (2.1), such that the existence of sufficiently many solutions mod $\mathscr{P}$ for all $\mathscr{P}$ with $M < \text{Norm}(\mathscr{P}) < P$ guarantees the algebraicity of all solutions of (2.1).

The main part in the proof of Theorem 2.2 is a special scheme of random walk on a zero-set for functions approximating solutions of linear differential equations (2.1). Remarkably, a random walk that we consider takes place on the standard tessellation of the upper half-plane by the action of full modular group $SL_2(\mathbb{Z})$, or of one of its congruence subgroups.

According to a "non-Euclidean" scheme of the random walk, a particle travels in the upper half-plane H, and at any moment of time a particle can change its current position z_i to $Tz_i = (az_i + b)/(cz_i + d)$ for $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, where $Tz_i = z_{i+1}$ lies in a circular triangle in H adjoint to the one containing z_i. For the full modular group $\Gamma(1) = SL_2(\mathbb{Z})$, there are three adjoint triangles. In general, for a given (congruence) subgroup G of $\Gamma(1)$ one covers H with images of the fundamental domain of G by the action of Möbius transformations from G. (See Fig. 1.)

In order to use a non-Euclidean random walk on modular domains, one needs a uniformization of solutions of a linear differential equation by means of appropriate modular functions in the upper half-plane. In the classical literature on the uniformization problem there is a body of papers devoted to the uniformization of solutions of the Fuchsian linear differential equations in terms of automorphic functions corresponding to Fuchsian (and sometimes Kleinian) group [13, 14]. In view of the well known problem

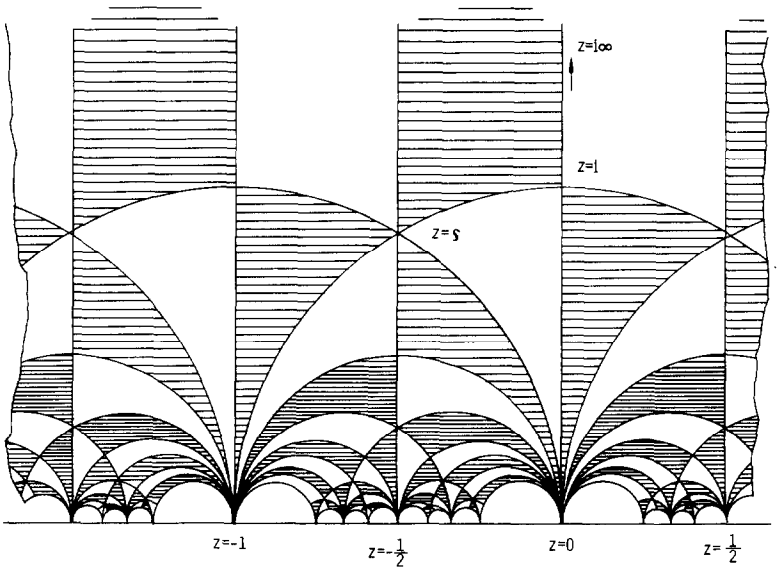

FIGURE 1

of accessory parameters [15] it is preferable to use a simpler and different uniformization approach. Since our main purpose is to uniformize an independent variable x by means of modular functions, it is sufficient to uniformize a dependent variable y by means of a function defined everywhere in the upper half-plane, whose modular properties are the reflection of the monodromy properties of Eq. (2.1). To do this, one needs to represent a multivalued function y as a multivalued function having only three regular singularities, say, $\{0, 1, \infty\}$, as those of inverses of classical automorphic functions for the full modular group and (some of) its principal congruence subgroups [16]. Such a representation of the Riemann surface of y, if possible at all, should lead to a differential equation of an order higher than that of (2.1), and to a representation of the monodromy group of (2.1) (or, rather, of its extension) in a higher dimensional space. Interestingly enough, a reduction (or, rather, a lifting) of the Fuchsian linear differential equation (2.1) is possible when (and only when) the differential equation (2.1) has its polynomial coefficients defined over an algebraic number field (!). Thus, in the framework of the Grothendieck conjecture, we can reduce Fuchsian linear differential equations to Fuchsian linear differential equations with three regular singularities $\{0, 1, \infty\}$ only, and then uniformize solutions of these equations by means of functions defined everywhere in

the upper half-plane. The basis for such reduction is the following startling result of Belyi [10]:

THEOREM 2.3 [10]. *A complete nonsingular algebraic curve, defined over a field of characteristic zero, can be represented as a covering of a projective line with the branch points at* $\{0, 1, \infty\}$ *only, if and only if this curve can be defined over an algebraic number field.*

A remarkably simple proof of Theorem 2.3 was based on the following observation:

LEMMA 2.4. *For an arbitrary finite set* X *of algebraic numbers there exists two nonzero polynomials* $p_X(x)$ *and* $q_X(x)$ *with rational number coefficients such that the following conditions are satisfied. First of all,* $p_X(x)$ *is branching only over rational numbers, i.e.,* $p_X(x_0) \in \mathbb{Q}$ *whenever* $p'_X(x_0) = 0$, *and* $q_X(z)$ *is branching only over* $\{0, 1, \infty\}$, *i.e.,* $q_X(x_0) = 0, 1$, *whenever* $q'_X(x_0) = 0$. *Secondly,* $p_X(x_1) \in \mathbb{Q}$ *whenever* $x_1 \in X$, *and* $q_X(x_1) = 0, 1$, *whenever* $x_1 \in X$ *and* $x_1 \in \mathbb{Q}$.

Proof. If $p_1(x)$ is a minimal polynomial defined over $\mathbb{Z}$ for all points of X, then we define inductively $p_{i+1}(x)$ as a minimal polynomial for the following set of algebraic numbers: $\{p_i(x_0): p'_i(x_0) = 0\}$. Since $\deg(p_{i+1}) < \deg(p_i)$, we have $p_{n+1} = \text{const}$ for some $n \geq 0$. Then we can put $p_X(x) \overset{\text{def}}{=} p_n(p_{n-1}(\ldots(p_1(x))\ldots))$. Let us construct now $q_X(x)$ for a set X of three rational numbers. If, say, $X = \{0, 1, s\}$ for $0 < s < 1$ and $s = m/(m+n)$ for integers m, n: $m \geq 0$, $n \geq 0$, then we can put

$$q_X(x) \overset{\text{def}}{=} \frac{(m+n)^{m+n}}{m^m \cdot n^n} x^m (1-x)^n.$$

Then by induction we can define $X = Y \cup \{x_0\}$, $X_0 = \{0, 1, q_Y(x_0)\}$ and put $q_X(x) \overset{\text{def}}{=} q_{X_0}(q_Y(x))$.

It seems that the (minimal) degrees of $p_X(x)$ and $q_X(x)$ grow at least linearly with the height of (elements of) X. As the proof of Lemma 2.4 shows, the most interesting case is that of X consisting of three distinct rational numbers; and in this case we present below a few examples associated with automorphic forms for congruence subgroups. In connection with these examples we remark that the degrees of $p_X(x)$ and $q_X(x)$ can be decreased, if to allow them to be rational functions with rational function coefficients.

Lemma 2.4 provides a immediate proof of Theorem 2.3. In fact, the "only if" part of the theorem is a trivial corollary of the Riemann existence theorem. If, on the other hand, a curve is defined over $\overline{\mathbb{Q}}$, then there exists at least one nonconstant rational function f on this curve, defining a covering

of $\mathbb{P}^1$ over $\overline{\mathbb{Q}}$ with a set S of branching points from $\overline{\mathbb{Q}}$ too. If we consider a polynomial $p_S(x)$ from Lemma 2.4 and define by X a set (of rational numbers) consisting of points $p_S(x_0)$ for $x_0 \in S$ and points $p_S(x_0)$ for $p_S'(x_0) = 0$, then the function $q_X(p_S(f))$ is a rational function on an algebraic curve, defining its covering over $\mathbb{P}^1$ with the branching points over $\{0, 1, \infty\}$ only.

Similar arguments can be used in the reduction of a Fuchsian linear differential equation, defined over $\overline{\mathbb{Q}}(x)$, to a Fuchsian linear differential equation defined over $\overline{\mathbb{Q}}(x)$ with regular singularities at $\{0, 1, \infty\}$ only.

Let us start from the polynomial from of a linear differential equation (2.1), where all $a_i(x)$ are polynomials from $\overline{\mathbb{Q}}(x)$: $i = 0,1,\ldots, n$. Zeroes of $a_n(x)$ are exactly the singularities of (2.1). Let us denote by S the set of all singularities of (2.1) (they are algebraic numbers). If, as above, $X = \{p_S(x_0)$: $p_S'(x_0) = 0$ on $x_0 \in S\}$, then we put $\varphi(x) \stackrel{\text{def}}{=} q_X(p_S(x))$. Let us denote by m the degree of the polynomial $\varphi(x)$. We now change the independent variable x to

$$x' = \varphi(x). \tag{2.3}$$

This change of variables geometrically represents a covering of degree m of $\mathbb{P}^1_{x'}$ with branch points at most at $\{0, 1, \infty\}$. This covering gives rise to m branches of x, considered as an algebraic function of x'. Let us denote these m branches by $x_\alpha = x_\alpha(x')$: $\alpha = 1,\ldots, m$.

We make a change (2.3) of an independent variable in the differential equation (2.1). This way we obtain a linear differential equation of nth order with algebraic function coefficients. This linear differential equation with algebraic coefficients can be, in its turn, reduced to a linear differential equation of order at most nm, having rational function coefficients and only $\{0, 1, \infty\}$ as its singular points. Indeed, let $y_1(x),\ldots, y_n(x)$ be an arbitrary fundamental system of solutions of (2.1). Let us introduce the following system of nm functions of a new variable x':

$$y_{i,j}(x') = y_i\big(x_j(x')\big): \qquad i = 1,\ldots, n;\ j = 1,\ldots, m.$$

First of all, the system of functions $Y = \{y_{i,j}(x')$: $i = 1,\ldots, n;\ j = 1,\ldots, m\}$ represents a complete system of solutions of a Fuchsian linear differential equation with rational function coefficients. Indeed, all singularities of functions from Y are regular, because they are regular for y_i and for x_j. Also an analytic continuation along any closed path of any function from Y is a linear combination of functions from Y again, because the same property holds for $\{y_1(x),\ldots, y_n(x)\}$ and an analytic continuation along the closed path in x' plane leads to a permutation of $x_\alpha(x')$. Also since (2.1) and (2.3) are defined over $\overline{\mathbb{Q}}$, a Fuchsian linear differential equation

satisfied by functions from Y has coefficients from $\overline{\mathbb{Q}}(x')$. All functions $x_\alpha(x')$ are regular everywhere but at $x' = 0, 1, \infty$. Hence a function from Y can have a singularity at a point $x' = x'_0$ only when $x_\alpha(x'_0) \in S$ (i.e., $x_\alpha = x_\alpha(x'_0)$ is a singularity of (2.1)). However, if $x_\alpha \in S$, then $\varphi(x_\alpha) = x'$ is 0, 1, or ∞, according to the properties of a polynomial $\varphi(x)$. Consequently, the only singularities of functions from Y are 0, 1, and ∞. Thus we obtain

THEOREM 2.5. *Every Fuchsian linear differential equation defined over* $\overline{\mathbb{Q}}(x)$ *can be reduced to a Fuchsian linear differential equation over* $\overline{\mathbb{Q}}(x')$ *with singularities at* $x' = 0, 1, \infty$ *only by an algebraic change of an independent variable. More precisely, there exists a change of variables* $x' = \varphi(x)$, *where* $\varphi(x)$ *is a polynomial with rational number coefficients, such that every solution* $y(x)$ *of a linear differential equation* (2.1) *is, as a function of* x', *a solution of a Fuchsian linear differential equation over* $\overline{\mathbb{Q}}(x')$ *with singularities only at* $x' = 0, 1, \infty$.

Remark 2.6. In the statement of Theorem 2.5, we can remove everywhere the word "Fuchsian."

Clearly, Theorem 2.3 is a particular case of Theorem 2.5, if applied to a Fuchsian linear differential equation satisfied by an arbitrary rational function on an algebraic curve defined over $\overline{\mathbb{Q}}$.

To see the expression of a reduction of an arbitrary linear differential equation over $\overline{\mathbb{Q}}(x)$ to the one having only 0, 1, and ∞ as its singularities, we can use elementary algebra. We employ the properties of the substitution (2.3). It is easier to consider a matrix first order linear differential equation over $\mathbb{Q}(x)$, equivalent to (2.1). Let this equation have the form

$$\frac{dy_i}{dx} = \sum_{j=1}^{n} A_{i,j}(x) y_j(x): \qquad i = 1, \ldots, n \tag{2.4}$$

for $A_{i,j}(x) \in \overline{\mathbb{Q}}(x)$ $(i, j = 1, \ldots, n)$. Let $D(x) \in \overline{\mathbb{Q}}[x]$ be a polynomial such that $D(x)A_{i,j}(x) \in \overline{\mathbb{Q}}[x]$ for all $i, j = 1, \ldots, n$. Zeroes of $D(x)$ are the singularities of (2.4). Note that the singularities of the equivalent systems (2.4) and (2.1) need not be the same: they may differ by apparent singularities, though regular singularities (and essential singularities) are the same. If (2.4) is a system of Fuchsian linear differential equations and all zeroes of $D(x)$ are simple ones, then (2.4) has normal or Schlesinger form [17].

Starting from an arbitrary solution $\mathbf{y}(x) = (y_1(x), \ldots, y_n(x))$ of (2.4), we introduce an nm-vector $\mathbf{Y}(x') = (y_i(x) \cdot x^j: i = 1, \ldots, n; j = 0, \ldots, m - 1)$, considered as a vector-function of x'. We show that $\mathbf{Y}(x')$ satisfies a matrix first order linear differential equation over $\overline{\mathbb{Q}}(x')$ with regular

singularities at $x' = 0, 1, \infty$ only. Indeed, $\varphi'(x) \cdot (dx/dx') = 1$ and

$$\frac{d}{dx'}\left(y_i(x) \cdot x^j\right) = \varphi'(x)^{-1} \cdot \left\{\frac{dy_i}{dx} \cdot x^j + y_i \cdot j \cdot x^{j-1}\right\}$$

$$= \left\{\sum_{k=1}^{n} A_{i,k}(x) x^j y_k + y_i \cdot j \cdot x^{j-1}\right\} \Big/ \varphi'(x).$$

Now, according to the properties of $\varphi(x)$, $D(x)$ divides $\varphi(x) \cdot (\varphi(x) - 1)$ and $\varphi'(x)$ divides $\varphi(x) \cdot (\varphi(x) - 1)$. Without the loss of generality we can assume that $D(x) \cdot \varphi'(x)$ divides $\varphi(x) \cdot (\varphi(x) - 1)$. Thus

$$x'(x' - 1)\frac{d}{dx'}\left(y_i(x) \cdot x^j\right)$$

$$= \frac{\varphi(x)(\varphi(x) - 1)}{D(x)\varphi'(x)} \cdot \left\{\sum_{k=1}^{n} B_{i,j,k}(x) \cdot y_k(\alpha)\right\},$$

where

$$B_{i,j,k}(x) \in \overline{\mathbf{Q}}[x]: \qquad i, k = 1, \ldots, n;\ j = 0, \ldots, m - 1.$$

Since $\varphi(x)(\varphi(x) - 1)/(D(x)\varphi'(x)) \in \overline{\mathbf{Q}}[x]$ and, according to the identity (2.3), any power x^r for $r = m, m + 1, \ldots$ can be expressed polynomially in x', we obtain

$$x'(x' - 1)\frac{d}{dx'}\left(y_i(x) \cdot x^j\right) = \sum_{l=0}^{m-1} \sum_{k=1}^{n} C_{i,j,k,l}(x') \cdot y_k(x) \cdot x^l$$

for $C_{i,j,k,l}(x') \in \overline{\mathbf{Q}}[x']$: $i, k = 1, \ldots, n$; $j, l = 1, \ldots, m$. Thus $\mathbf{Y}(x')$ satisfies a first order matrix linear differential equation of the form

$$x'(x' - 1)\frac{d\mathbf{Y}}{dx'} = C(x') \cdot \mathbf{Y}(x') \tag{2.5}$$

for $C(x') \in M_{nm}(\mathbf{Q}[x'])$. If the original matrix equation (2.4) is Fuchsian (of the normal form [17]), then the resulting equation (2.5) is again Fuchsian (and of the normal form). We can reformulate this as a

COROLLARY 2.7. *Every matrix linear differential equation of the normal form*

$$\frac{dY}{dx} = \left(\sum_{i=1}^{k} \frac{U_i}{x - \alpha_i} + U_0\right) Y$$

for $\alpha_i \in \overline{\mathbf{Q}}$, $U_i \in M_n(\overline{\mathbf{Q}})$ $(i = 0, \ldots, k)$ *can be reduced, by a polynomial change* $x' = \varphi(x)$ *of an independent variable, to a matrix linear differential equation in the normal form having singularities only at* $x = 0, 1, \infty$:

$$\frac{dY_1}{dx'} = \left(\frac{A}{x'} + \frac{B}{x' - 1} + C\right) Y_1 \tag{2.6}$$

with $A, B, C \in M_{nm}(\overline{\mathbf{Q}})$ *for* $m = \deg(\varphi)$.

Corollary 2.7 (or Theorem 2.5) allows us to express solutions of arbitrary (Fuchsian) linear differential equations over $\overline{\mathbf{Q}}(x)$ in terms of single-valued functions in the upper half-plane, and to study monodromy of these differential equations from the point of view of Möbius transformations corresponding to matrices from the modular group $\Gamma(1) = SL_2(\mathbf{Z})$. A reference to the possibility of such expression, once a linear differential equation is represented in the form (2.6), can be found in Baker [18].

Following [18], we consider an automorphic function $k^2(z)$ for the group $\Gamma(2)$. It is known that $k^2 = (\theta_2^4(0;q))/(\theta_3^4(0;q))$ and $1 - k^2 = (\theta_4^4(0;q))/(\theta_3^4(0;q))$ for $q = e^{\pi i z}$. The function z, inverse to $k^2(z)$, is represented by the ratio of hypergeometric functions (periods of the elliptic integral with the invariant k^2):

$$z = i \cdot \frac{F(1 - k^2)}{F(k^2)},$$

where $F(t) = (2/\pi)\int_0^{\pi/2}(1 - t\sin^2\theta)^{-1/2}\,d\theta = \sum_{n=0}^{\infty}\binom{2n}{n}^2(t/4)^n$. Two functions $\log(k^2)$ and $\log(1 - k^2)$ are represented as series in q. Thus we can denote

$$\log(k^2) = \psi(z), \qquad \log(k^2 - 1) = \psi_1(z),$$

i.e., $k^2 = e^{\psi(z)}$, for single-valued functions $\psi(z)$, $\psi_1(z)$ in H. Thus, if we make a natural change of the independent variable $x' = k^2(z)$, the matrix differential equation (2.6) is reduced to the following one

$$\frac{dY_1}{dz} = \left(A \cdot \psi'(z) + B \cdot \psi_1'(z) + C \cdot \psi'(z) \cdot e^{\psi(z)}\right) Y_1. \tag{2.7}$$

Since coefficients of (2.7) are integral functions in H, the results of Baker [19] show that elements of the solution Y_1 of (2.7) are single-valued functions of z in H. An independent proof of this follows from Theorem 2.5 and properties of z as a function of $k^2(z)$, having singularities only at $0, 1, \infty$. More elaborate transformations would allow us to use the automorphic function $J(z)$ for $\Gamma(1)$ instead of $k^2(z)$ (use, say, the expression

$$J(z) = 4(1 - k^2 + k^4)^3/\left(27k^4(1 - k^2)^2\right)\ ).$$

Such a transformation allows us to simplify the study of the effect of the monodromy transformations (as a result of an analytic continuation along a closed path) for the original linear differential equation. First of all, the monodromy of the reduced equation (2.6) is expressed explicitly in terms of the monodromy of the original equation (2.4), and the matrices of the monodromy group (or, rather, of its representation) of (2.6) are built from monodromy matrices of (2.4) and from the matrices representing the Galois group of the Riemann surface of $x' = \varphi(x)$. As a result, if the equation (2.3) is algebraically represented, i.e., its monodromy group is a subgroup of $GL_n(\overline{\mathbf{Q}})$ for some choice of the basis, then the reduced equation (2.6) is also algebraically represented.

To study the effect of the monodromy transformation of the equation (2.6) in terms of a new variable z in H, $x' = k^2(z)$ let us consider an arbitrary closed path γ in $\mathbf{CP}^1_{x'}$, not containing 0, 1, or ∞. An analytic continuation along γ from x' to x' is equivalent in H to a transformation $z \mapsto T_\gamma \cdot z = (a_\gamma z + b_\gamma)/(c_\gamma z + d_\gamma)$ with integers $a_\gamma, b_\gamma, c_\gamma, d_\gamma$ such that $a_\gamma d_\gamma - b_\gamma c_\gamma = 1$, even b_γ, c_γ and odd a_γ, d_γ. The group $\Gamma(2)$ of fractional transformations T_γ is generated by two transformations $z'\ (= \sigma(z)) = z + 2$ and $z'\ (= \tau(z)) = z/(2z + 1)$. To see the effect of analytic continuation along γ, let z be a (unique) element of the fundamental domain F_2 of $\Gamma(2)$ such that $x' = k^2(z)$: $\operatorname{Im} z > 0$, $|z - 1/2| \geq 1/2$, $-1 \leq \operatorname{Re} z < 1$. Then analytic continuation of Y_1 along γ from x' to x' manifests itself in H by a reflection of z to $z' = T_\gamma z$ by successive reflections from F_2 to its doubles adjoint to each other. As a result of these transformations, $x' = k^2(z')$, according to the automorphicity conditions. The matrix function $Y_1 = Y_1(z)$ undergoes a linear transformation $Y_1 \mapsto Y_1 \cdot M_\gamma$ for a matrix $M_\gamma \in GL_n(\mathbf{C})$ from the monodromy group of (2.6), corresponding to the transformation T_γ. As $\Gamma(2)$, the monodromy group of (2.6) is generated by two matrices M_σ and M_τ corresponding to two transformations σ and τ of $\Gamma(2)$. In particular, if M_σ and M_τ are both matrices with algebraic entries, the equation (2.6) is algebraically represented.

In application to the Grothendieck conjecture we consider the case when an original system (2.4) is algebraically represented and has a matrix solution $Y(x)$, whose elements are (convergent) power series from $\overline{\mathbf{Q}}[[x]]$ that have integral (or nearly integral) coefficients. According to the Eisenstein's theorem, the same property holds for the matrix solution $Y_1(x')$ of (2.6). Moreover, the algebraic representation of (2.6) implies that an arbitrary modular transformation T_γ of H leads to the transformed matrix function $Y_1 \cdot M_\gamma$, all elements of which are again power series with integral (or nearly integral) coefficients from $\overline{\mathbf{Q}}$.

The near integrality of the power series expansions of solutions of a linear differential equation (2.1) or (2.4), if all assumptions of the Grothendieck conjecture are satisfied, is the crucial property in the proof Theorem 2.2. We

use here results of Section 2 of [9]. According to Corollary 2.5 of [9], let the equation (2.1) satisfy the assumptions of the Grothendieck conjecture, and let $y(x) = \sum_{m=0}^{\infty} c_m (x - \xi)^m$ be a solution of (2.1) with an algebraic ξ, and initial conditions $y^{(i)}(\xi) = i! \cdot c_i$ for algebraic numbers c_i: $i = 0, \ldots, n-1$. Let us put $y(x)^j = \sum_{m=0}^{\infty} c_{m,j}(x - \xi)^m$, $j = 1, 2, \ldots$. Then the common denominator of numbers $\{c_{m_1} \ldots c_{m_j}: m_1 + \cdots + m_j \le M: j = 1, \ldots, k\}$ and the common denominator of numbers $\{c_{m,j}: m = 0, 1, \ldots, M; j = 1, \ldots, k\}$ both divide the number $\Delta_{M;k}$, where $\log|\Delta_{M;k}| \le M \log c_1 + k \log c_2$, where c_2 depends only on $y(x)$, and c_1 depends effectively on (2.1), ξ, and the (finite) set of primes p, for which (2.1) has a nonzero p-adic curvature.

The proof of Theorem 2.2 proceeds along the lines indicated in Section 1, and is very similar in its algebraic part to the proofs from [8, 9]. First of all, we reduce Eq. (2.1) or (2.2) to the form (2.6), where the dependent and independent variables are parametrized by functions in z uniform in H. As we already noted, the near integrality property of the coefficients in the expansion of solutions of linear differential equations does not change if we pass from (2.1) or (2.2) to (2.6). Let us consider an arbitrary solution $\mathbf{Y}(x') = (y_1(x'), \ldots, y_k(x'))$ of (2.6), having algebraic initial conditions. An auxiliary approximation function, as in Section 1, has the form

$$F(x') = P(x', y_1(x'))$$

for a nonzero polynomial $P(x', y') \in \mathbb{Z}[x', y']$. By means of the uniformization in H, we obtain a function $f(z) = F(x')$, where $x' = k^2(z)$ (or $x' = J(z)$) and $y_1(x') = \varphi(z)$ is a single-valued function on H. The polynomial $P(x', y')$ is defined in a way that the corresponding function $f(z)$ has zeroes of high order at points of a large zero-set $z_0, \ldots, z_i, z_{i+1} = T_i z_i, z_{i+2}, \ldots$ (where $z_0 \in F_2$ corresponds to the point $x' = \xi$, where the expansions of $y_i(x')$ are nearly integral: $i = 1, \ldots, k$). The monodromy transformations of (2.6) generate, as it was shown before, transformations $z_i \to z_{i+1}$ and lead to new functions $y_{1,i}(x')$ corresponding to $\varphi(z_i)$. The algebraic representation of (2.6) implies that all expansions of $y_{1,i}(x)$ at $x' = \xi$ are nearly integral again. Thus, the denominators of all numbers $(1/m!)(d/dx')^m\{P(x', y_{1,i}(x'))\}|_{x=\xi}$ corresponding to $(1/m!)(d/dz)^m \cdot \varphi(z_i)$, are easily controllable as in [8, 9] or the theory of G-functions. Hence, we arrive, as in Section 1, to the system of Markov-type inequalities on the orders of zeroes of $\varphi(z_i)$, similar to (1.6). This system determines a scheme of non-Euclidian random walk on H. In the estimates of the growth of $(1/m!)(d/dz)^m\varphi(z_i)$, we use the properties of $\Gamma(1)$ and that of $\sum|z_i|^\nu$ and $\prod(z - z_i^*)/(z - z_i)$ for $z \in H$. Similar to Section 1, we arrive at an excessive function on a random walk lattice $\{z_i\}$ in H, which can exist only in a bounded domain. Apparent contradiction forces $\varphi(z) \equiv 0$ and $y_1(x')$

becomes an algebraic function. Details of the proof of Theorem 2.2 will be presented elsewhere.

While the Theorem 2.2 is a transcendence statement in function theory, its random walk proof show that it leads to a statement on transcendental numbers. Namely, if $y = (y_1(x'), \ldots, y_k(x'))$ is a transcendental G-function solution [11] of a matrix linear differential equation (2.6) over $\bar{\mathbf{Q}}(x')$ with algebraic initial conditions at $x' = \xi \neq 0, 1, \infty$, then among all analytic continuations $(y_1^{(\gamma)}, \ldots, y_n^{(\gamma)})$, of y from ξ to ξ along the closed paths γ in $\mathbf{CP}^1$, there exists at least one transcendental number $y_i^{(\gamma)}$.

We conclude this section with some explicit formulas related to the reduction Theorem 2.6. Our examples are connected with the problem of explicit computations of accessory parameters, i.e., with the problem of an effective computation of a monodromy group of a linear differential equation in terms of parameters in the coefficients of the differential equation. Theorem 2.6 allows us to reduce a linear differential equation to the one with singularities at $0, 1, \infty$ only. Therefore, if the resulting linear differential equation is of hypergeometric type (again only with regular singularities at $0, 1, \infty$), then the monodromy group of the original equation will be explicitly known. This method can be reformulated in the form of lifting of hypergeometric function equations to equations of higher order by means of polynomial (rational) transformations. If one restricts oneself to the first nontrivial case of the accessory parameter problem of the Lamé equation in the transcendental form $d^2w/dz^2 + (1/4)(\mathcal{P}(z) + B)w = 0$, it turns out that the investigation of this case was conducted by Smirnov [20]. By means of linear and quadratic transformations, the Lamé equation can be represented in the algebraic form as an equation with four regular singularities at $x = a_1, a_2, a_3$, and ∞ and with equal roots of the indicial equation at every regular singularity. The canonical form of this equation is

$$\frac{d}{dx}\left[(x - a_1)(x - a_2)(x - a_3)\frac{dy}{dx}\right] + (x + A)y = 0, \tag{2.8}$$

where A is an accessory parameter. According to the study of [20], an equation (2.8) can be reduced to the Gauss hypergeometric equation by means of rational transformation

$$x' = r(x) \tag{2.9}$$

only in finitely many cases, the most general of which are the cases when: (1) values $x = 0, 1, t, \infty$ and only they give $x' = 0$; (2) all roots of $r(x) = \infty$ have the multiplicity n and all roots of $r(x) = 1$ have the multiplicity m; and (3) no other values of x, than those in (1)–(2) give the multiple root in (2.9). Integers n and m in (1)–(3) can have only finitely many values. The number of all possible rational transformations (2.9) reducing (2.8) to the

hypergeometric form is limited, but large. A computer check of all of them reveals that up to a trivial transformation there are only five equations (2.8) that can be reduced to the Gauss form. The leading coefficient $f(x) = (x - a_1)(x - a_2)(x - a_3)$ of (2.8) can be reduced to one of the following four forms:

$$f(x) = x^3 - 1, \qquad x(x^2 - 1),$$
$$x(x^2 + 11x - 1), \qquad x(8x^2 + 7x - 1). \tag{2.10}$$

In the four cases of (2.10), it is easy to compute the value of an accessory parameter A, for which (2.8) reduces to the hypergeometric form. In this case the monodromy group of (2.8) can be explicitly computed, and, in fact, coincides with one of the congruence subgroups of $\Gamma(1)$. This is not accidental, because transformations (2.9) in the cases (2.10) are particular examples of modular transformations from [16] corresponding to the modular curves of genus zero and their uniformizations in rational functions. Other rational uniformizations from [16] (e.g., [16], Chap. IV.2]) lead to differential equations with more than four singularities. A simple structure of the monodromy of equations (2.8) in cases (2.10) provides additional arithmetic information on equations (2.8) in cases (2.10), namely, their p-curvature operators (see above) are nilpotent. This implies the near integrality of solutions of (2.8). Since coefficients of the expansions of a solution of (2.8) at $x = a_i$ satisfy three-term recurrences, we arrive at integral (nearly integral) solutions of three-term recurrences. All these solutions are, in fact, known! It turns out that the cases (2.10) of (2.8) are related with Apéry sequences approximating $\zeta(2)$ and $\zeta(3)$, as described in a very interesting paper of Dwork [21], where the relationship with the p-adic linear differential equations is presented. In fact, the two last cases in (2.10) correspond to linear differential operators L_1 and L_2 in 4.1 and 4.2 [21]. The third operator, L_3 of 4.3 [21], corresponding to Apéry approximation to $\zeta(3)$, is a symmetric square of the operator L_4 [21], and the quadratic transformation reduces L_4 to the equation (2.8) for the last case in (2.10).

REFERENCES

1. P. CASSOU-NOGUES, Valeurs aux entiers négatifs des séries de Dirichlet associées à un polynôme II, *Amer. J. Math.* **106** (1984), 255–299.
2. G. V. CHUDNOVSKY, A new method for the investigation of arithmetical properties of analytic functions, *Ann. Math.* **109** (1979), 353–377.
3. G. V. CHUDNOVSKY, Singular points on complex hypersurfaces and multidimensional Schwarz lemma, Seminaire Delange–Pisot–Poitou, 19e annee 1977/78, *in* "Progress in Mathematics," Vol. 12, pp. 29–69, Birkhauser, Boston, 1981.
4. D. V. CHUDNOVSKY AND G. V. CHUDNOVSKY, Padé approximations to solutions of linear differential equations and applications to diophantine analysis, *in* "Number Theory," New

York 1984, Lecture Notes in Math., Vol. 1052, pp. 85–167, Springer-Verlag, New York, 1984.
5. E. B. DYNKIN AND A. A. YUSHKEVICH, "Markov Processes: Theorems and Problems," Plenum, New York, 1969.
6. N. KATZ, A conjecture in the arithmetic theory of differential equations, *Bull. Soc. Math. France* **110** (1982), 203–239, corr. 347–348.
7. T. HONDA, Algebraic differential equations, *in* "Symposia Mathematica," Vol. 24, pp. 169–204, Academic Press, New York, 1981.
8. D. V. CHUDNOVSKY AND G. V. CHUDNOVSKY, The Grothendieck conjecture and Padé approximations, *Proc. Japan Acad.* **61**A (1985), 87–91.
9. D. V. CHUDNOVSKY AND G. V. CHUDNOVSKY, Applications of Padé approximations to the Grothendieck conjecture on linear differential equations, *in* "Number Theory," New York 1984, Lecture Notes in Math., Vol. 1135, pp. 52–100, Springer-Verlag, New York, 1985.
10. G. V. BELYI, On Galois extensions of a maximal cyclotomic field, *Izv. Akad. Nauk SSSR. Mat.* **43** (1979), 267–276; English Transl. in *Math. USSR Izv.* **14** (1980), 247–256.
11. D. V. CHUDNOVSKY AND G. V. CHUDNOVSKY, Applications of Padé approximations to diophantine inequalities in values of G-function, *in* "Number Theory," New York, 1984, Lecture Notes in Math., Vol. 1135, pp. 9–51, Springer-Verlag, New York, 1985.
12. E. BOMBIERI AND S. LANG, Analytic subgroups of group varieties, *Invent. Math.* **11** (1970), 1–14.
13. H. POINCARÉ, Sur les groupes des équations linéaires, *Acta Math.* **4** (1884), 201–312.
14. A. R. FORSYTH, "Theory of Differential Equations," Vol. 4, Cambridge Univ. Press, London/New York, 1902.
15. D. S. HEJHAL, Monodromy groups and linearly polymorphic functions, *Acta. Math.* **135** (1975), 1–55.
16. F. KLEIN AND R. FRICKE, Vorlesungen über die Theorie der elliptischen Modulfunktionen, Vol. 2, Teubner, Stuttgart, 1892.
17. G. V. CHUDNOVSKY, Rational and Padé approximations to solutions of linear differential equations and the monodromy group, *in* "Proceedings of the 1979 Les Houches International Colloquium on Complex Analysis and Relativistic Quantum Field Theory," Lecture Notes in Physics, Vol. 126, pp. 136–169, Springer-Verlag, New York, 1980.
18. H. F. BAKER, Notes introductory to the study of Klein's group of order 168, *Proc. Cambridge Philos. Soc.* **31** (1935), 468–481.
19. H. F. BAKER, On the integration of linear differential equations, *Proc. London Math. Soc.* **35** (1903), 333–378.
20. V. I. SMIRNOV, On rational transformations of linear differential equations of the second order, *Math. Sbornik* **32** (1927), 101–106.
21. B. DWORK, Arithmetic theory of differential equations, *in* "Symposia Mathematica," Vol. 24, pp. 225–243, Academic Press, New York, 1981.